

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-125484

(P2001-125484A)

(43) 公開日 平成13年5月11日 (2001.5.11)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
G 0 9 C 5/00		G 0 9 C 5/00	5 B 0 5 7
G 0 6 T 1/00		G 1 0 H 1/00	Z 5 C 0 7 6
G 1 0 H 1/00		G 1 1 B 19/04	5 0 1 H 5 D 0 4 4
G 1 1 B 19/04	5 0 1	20/10	H 5 D 3 7 8
20/10		H 0 4 N 1/387	5 J 1 0 4

審査請求 未請求 請求項の数 5 O L (全 6 頁) 最終頁に続く

(21) 出願番号 特願平11-302095

(22) 出願日 平成11年10月25日 (1999. 10. 25)

(71) 出願人 000004329

日本ビクター株式会社

神奈川県横浜市神奈川区守屋町 3 丁目12番  
地

(72) 発明者 内藤 丈嗣

神奈川県横浜市神奈川区守屋町 3 丁目12番  
地 日本ビクター株式会社内

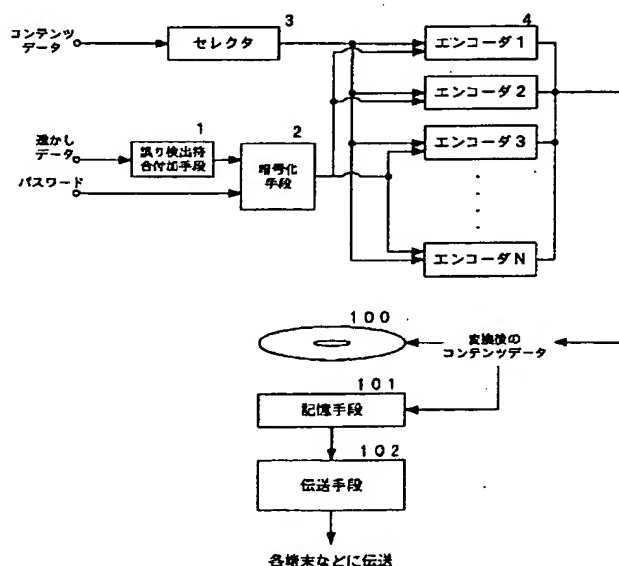
最終頁に続く

(54) 【発明の名称】 透かしデータ埋め込み装置、透かしデータ埋め込み方法、伝送方法、記録媒体、及び透かしデータ読み出し方法。

(57) 【要約】

【課題】 コンテンツデータに透かしデータを埋め込む際に、コンテンツデータの劣化を最小限にすると共に、第三者がコンテンツデータに埋め込まれた透かしデータだけを取り除くことを困難とする。

【解決手段】 透かしデータに対して誤り検出符合を付加し、更に、入力されたパスワードを基に誤り検出符合を付加された透かしデータを暗号化して得られた透かしデータを異なる強度の複数の埋め込み手段から一つの埋め込み手段を選択してコンテンツデータに埋め込みを行う。



## 【特許請求の範囲】

【請求項1】 コンテンツデータに埋め込む透かしデータに対して誤り検出符号を付加する誤り検出符号付加手段と、

入力されたパスワードを基に前記誤り検出符号を付加された透かしデータを暗号化する暗号化手段と、

前記コンテンツデータに対して前記暗号化された透かしデータを埋め込むためにそれぞれ異なる埋め込み強度を有する複数の透かしデータ埋め込み手段と、実際に透かしデータの埋め込みを行う埋め込み手段を前記複数の透かしデータ埋め込み手段から選択する埋め込み手段選択手段とを有することを特徴とする透かしデータ埋め込み装置。

【請求項2】 コンテンツデータに埋め込む透かしデータに対して誤り検出符号を付加するステップと、

パスワードを入力するステップと、

前記パスワードを基に前記誤り検出符号を付加した透かしデータを暗号化するステップと、

前記コンテンツデータに対して前記暗号化された透かしデータを埋め込むためにそれぞれ異なる埋め込み強度を有する複数の透かしデータ埋め込み手段の中から、実際に透かしデータの埋め込みを行う埋め込み手段を選択するステップと、

選択された埋め込み手段によって前記暗号化された透かしデータを埋め込むステップからなる透かしデータ埋め込み方法。

【請求項3】 コンテンツデータに埋め込む透かしデータに対して誤り検出符号を付加し、

入力したパスワードを基に前記誤り検出符号を付加した透かしデータを暗号化し、

前記コンテンツデータに対して前記暗号化された透かしデータを埋め込むためにそれぞれ異なる埋め込み強度を有する複数の透かしデータ埋め込み手段の中から、実際に透かしデータの埋め込みを行う埋め込み手段を選択し、選択された埋め込み手段によって前記暗号化された透かしデータを埋め込むことにより得られる透かしデータを埋め込んだ前記コンテンツデータを伝送することを特徴とする伝送方法。

【請求項4】 コンテンツデータに埋め込む透かしデータに対して誤り検出符号を付加し、

入力したパスワードを基に前記誤り検出符号を付加した透かしデータを暗号化し、

前記コンテンツデータに対して前記暗号化された透かしデータを埋め込むためにそれぞれ異なる埋め込み強度を有する複数の透かしデータ埋め込み手段の中から、実際に透かしデータの埋め込みを行う埋め込み手段を選択し、選択された埋め込み手段によって前記暗号化された透かしデータを埋め込むことにより得られる透かしデータを埋め込んだ前記コンテンツデータを記録することを特徴とする記録媒体。

【請求項5】 コンテンツデータに埋め込む透かしデータに対して誤り検出符号を付加し、

入力したパスワードを基に前記誤り検出符号を付加した透かしデータを暗号化し、

前記コンテンツデータに対して前記暗号化された透かしデータを埋め込むためにそれぞれ異なる埋め込み強度を有する複数の埋め込み手段から一つの埋め込み手段を選択して埋め込むことにより得られる透かしデータを埋め込んだ前記コンテンツデータに対して、

10 前記異なる埋め込み強度を有する複数の埋め込み手段に対応する全ての読み出し手段によって前記透かしデータを埋め込んだ前記コンテンツデータから透かしデータを読み出し、

読み出したそれぞれの透かしデータに対して前記パスワードを用いて復号化して、その結果の正当性を前記誤り検出することで確認し、

正当であると確認されたものを真の透かしデータとすることを特徴とする透かしデータ読み出し方法。

## 【発明の詳細な説明】

20 【0001】

【発明の属する技術分野】 デジタル化されたコンテンツデータを配信するシステムにおいて、コンテンツの違法コピー及び再販を防止するために、コンテンツの著作権などの製作者に関する情報を透かしデータ (digital watermark) として記録する透かしデータ埋め込み装置、透かしデータ埋め込み方法、透かしデータを埋め込んだデータを伝送する伝送方法、透かしデータを埋め込んだ記録媒体、及び透かしデータ読み出し方法に関するものである。

30 【0002】

【従来の技術】 デジタル技術の進歩により、映画、音楽、写真等の様々な著作物がデジタルデータとして流通されている。これらのデジタルデータは静止画や動画等の画像データや音声データ、MIDIデータのコンテンツデータがデジタル化されたもので、CD-ROM等の記録媒体に記録されて販売されたり、インターネット等のネットワークによって送受信されたりしている。

【0003】 このようなデジタルデータは、完全なコピーを容易に、しかも大量に作成できるという特徴を持ち、これは、そのデジタルデータを入手したユーザがオリジナルと同等のコピーを不正に作成して再配布、再販売できるという可能性を示している。これにより、デジタルデータの著作者又は著作者から正当に販売を委託された者に支払われるべき代価が支払われず、著作権が侵害されることがある。

【0004】 このようなデジタルデータからなる著作物の著作権を巡る問題が深刻になってきており、近年、これを防止するための技術として電子透かし技術が脚光を浴びてきている。

50 【0005】 この技術は、データの作成者、提供者等の

権利を保護するために、データの中に作成者や利用者に関する情報を、ユーザには判別できない形で挿入し、著作権者を確認したり、不正使用があった場合に、そのユーザを特定できるようにしたりするものである。

【0006】この電子透かしに必要な条件としては、①無理に透かしデータを取り去ろうとするとコンテンツデータ自体が壊れてしまうように透かしデータを埋め込むこと（コンテンツデータに著作権を示す透かし情報が残り続けること）、②コンテンツデータのどこに透かし情報が埋め込まれているかが分かり難いこと、③透かしデータを埋め込んでもコンテンツデータはオリジナルの状態、クオリティを留めておくこと等がある。

【0007】これらの条件を満たす電子透かし技術としては、画像データや音声データ等のコンテンツデータに存在する人間の知覚上重要ではない部分（冗長部分）に透かしデータを埋め込むことにより、全体のデータ量を変えずに透かしデータを埋め込むことが考えられている。

【0008】また、コンテンツデータのうち特定のデータに着目し、これら特定のデータの一部を他のデータに置き換えて電子透かしとする方法も考えられている。

【0009】

【発明が解決しようとする課題】しかしながら、コンテンツデータに透かしデータを埋め込む際に、どの程度の強度で透かしデータを埋め込むべきであるかを決定するのは難しい。これは、透かしデータの埋め込み強度を強くすればするほど、コンテンツデータへ及ぼす影響が大きくなり、結果的にコンテンツデータの劣化が大きくなるという問題があった。しかし、透かしデータの埋め込み強度を弱くしすぎると第三者が透かしデータを故意に取り除くことが比較的容易となってしまうという問題があった

【0010】

【課題を解決するための手段】そこで、本発明は、コンテンツデータに埋め込む透かしデータに対して誤り検出符号を付加する誤り検出符号付加手段1と、入力されたパスワードを基に前記誤り検出符号を付加された透かしデータを暗号化する暗号化手段2と、前記コンテンツデータに対して前記暗号化された透かしデータを埋め込むためにそれぞれ異なる埋め込み強度を有する複数の透かしデータ埋め込み手段4と、実際に透かしデータの埋め込みを行う埋め込み手段4を前記複数の透かしデータ埋め込み手段4から選択する埋め込み手段選択手段3とを有することを特徴とする透かしデータ埋め込み装置を提供する。

【0011】また、コンテンツデータに埋め込む透かしデータに対して誤り検出符号を付加するステップと、パスワードを入力するステップと、前記パスワードを基に前記誤り検出符号を付加した透かしデータを暗号化するステップと、前記コンテンツデータに対して前記暗号化

された透かしデータを埋め込むためにそれぞれ異なる埋め込み強度を有する複数の透かしデータ埋め込み手段の中から、実際に透かしデータの埋め込みを行う埋め込み手段を選択するステップと、選択された埋め込み手段によって前記暗号化された透かしデータを埋め込むステップからなる透かしデータ埋め込み方法を提供する。

【0012】更に、コンテンツデータに埋め込む透かしデータに対して誤り検出符号を付加し、入力したパスワードを基に前記誤り検出符号を付加した透かしデータを暗号化し、前記コンテンツデータに対して前記暗号化された透かしデータを埋め込むためにそれぞれ異なる埋め込み強度を有する複数の透かしデータ埋め込み手段の中から、実際に透かしデータの埋め込みを行う埋め込み手段を選択し、選択された埋め込み手段によって前記暗号化された透かしデータを埋め込むことにより得られる透かしデータを埋め込んだ前記コンテンツデータを伝送することを特徴とする伝送方法を提供する。

【0013】また更に、コンテンツデータに埋め込む透かしデータに対して誤り検出符号を付加し、入力したパスワードを基に前記誤り検出符号を付加した透かしデータを暗号化し、前記コンテンツデータに対して前記暗号化された透かしデータを埋め込むためにそれぞれ異なる埋め込み強度を有する複数の透かしデータ埋め込み手段の中から、実際に透かしデータの埋め込みを行う埋め込み手段を選択し、選択された埋め込み手段によって前記暗号化された透かしデータを埋め込むことにより得られる透かしデータを埋め込んだ前記コンテンツデータを記録することを特徴とする記録媒体100を提供する。

【0014】また、コンテンツデータに埋め込む透かしデータに対して誤り検出符号を付加し、入力したパスワードを基に前記誤り検出符号を付加した透かしデータを暗号化し、前記コンテンツデータに対して前記暗号化された透かしデータを埋め込むためにそれぞれ異なる埋め込み強度を有する複数の埋め込み手段から一つの埋め込み手段を選択して埋め込むことにより得られる透かしデータを埋め込んだ前記コンテンツデータに対して、前記異なる埋め込み方法を有する複数の埋め込み手段に対応する全ての読み出し手段によって前記透かしデータを埋め込んだ前記コンテンツデータから透かしデータを読み出し、読み出したそれぞれの透かしデータに対して前記パスワードを用いて復号化して、その結果の正当性を前記誤り検出することで確認し、正当であると確認されたものを真の透かしデータとすることを特徴とする透かしデータ読み出し方法を提供する。

【0015】

【発明の実施の形態】以下、本発明に係る透かしデータ埋め込み装置、透かしデータ埋め込み方法、透かしデータを埋め込んだデータを伝送する伝送方法、透かしデータを埋め込んだ記録媒体、及び透かしデータ読み出し方法について図面を用いて説明する。

10

20

30

40

50

【0016】図1は本発明に係る透かしデータ埋め込み装置の概念を示すブロック図である。同図によれば、透かしデータは誤り検出符号付加手段1によって誤り検出符号を付加された後、暗号化手段2に送られ、暗号化手段2ではユーザーによって入力されたパスワードを基に暗号化される。

【0017】このように誤り検出符号を付加され、暗号化を施された透かしデータは、強度の異なるN個の透かし埋め込み用のエンコーダ4によってコンテンツデータに埋め込まれる。このエンコーダ4は異なる強度の透かし埋め込み方法を採用しており、このエンコーダ4の中からセクタ3によって任意に、又はランダムに選択されて透かしデータの埋め込みが行われる。

【0018】ここで、上述した異なる強度の透かし埋め込み方法の一例を16ビットに量子化されたサンプルデータに透かしを埋め込む場合を基に説明する。異なる透かし埋め込み強度を有する4個のエンコーダ4(N=4)を使用するが、第1のエンコーダの透かし埋め込み強度が最も弱く、第2のエンコーダの透かし埋め込み強度、第3のエンコーダの透かし埋め込み強度と順に透かし埋め込み強度が強くなっていき、第4のエンコーダの透かし埋め込み強度が最も強いものとする、基のコンテンツデータが次に示す16ビットのサンプルデータである場合に、

1001100100011110

第1のエンコーダによって透かしデータを埋め込まれたサンプルデータは次に示す通りとなる。

1001100100011110 (埋め込みビットが0の場合)

1001100100011111 (埋め込みビットが1の場合)

また、第2のエンコーダによって透かしデータを埋め込まれたサンプルデータは次に示す通りとなる。

1001100100011100 (埋め込みビットが0の場合)

1001100100011110 (埋め込みビットが1の場合)

更に、第3のエンコーダによって透かしデータを埋め込まれたサンプルデータは次に示す通りとなる。

1001100100011000 (埋め込みビットが0の場合)

1001100100011100 (埋め込みビットが1の場合)

また更に、第4のエンコーダによって透かしデータが埋め込まれたサンプルデータは次に示す通りとなる。

1001100100010000 (埋め込みビットが0の場合)

1001100100011000 (埋め込みビットが1の場合)

これらのエンコーダ4の中からセクタ3によって選択

されたエンコーダ4でコンテンツデータに透かしデータが埋め込まれる。このとき、透かし埋め込み強度を強くするに従って基のコンテンツデータに対する影響が大きくなっている。このような透かしデータの埋め込みを行ったコンテンツデータに対して第三者が透かしデータを除去すべく攻撃を行った場合、例えば、第1のエンコーダによって透かしデータを埋め込まれたコンテンツデータに対しては下位1ビットに対する攻撃で透かしデータを除去することが可能であるが(強度のみに着目した場合)、第4のエンコーダによって透かしデータを埋め込まれたコンテンツデータに対しては下位4ビットに対して攻撃しなければ透かしデータを除去することができない。すると、最も透かし強度の強い場合を想定して攻撃をしなければならず、攻撃後のコンテンツデータの品質劣化が大きくなってしまい、コンテンツデータとしての役割を果たせない場合も考えられる。

【0019】従って、コンテンツデータの重要度等によって透かしデータの埋め込みに使用するエンコーダを選択して透かしデータの埋め込み強度を任意に設定したり、ランダムに選択することで、コンテンツデータへの第三者からの攻撃を効率良く回避することが可能となる。

【0020】なお、本実施例では透かしデータの埋め込み強度をコンテンツデータの上位ビットに埋め込むに従って強くなるものとしており、それよりも下位のビットはノイズ成分として扱っているが、透かしデータの埋め込み強度についてはこれに限定されるものではないことはもちろんである。

【0021】以上のように、透かしデータを埋め込まれた変換後のコンテンツデータは必要に応じて記録媒体100に記録されたり、各端末などに伝送するために伝送手段102に接続された記憶手段101に記録されたりする。こうして、記録媒体100によって透かしデータを埋め込まれたコンテンツデータを頒布したり、伝送手段102によって透かしデータの埋め込まれたコンテンツデータを配信することが可能となる。

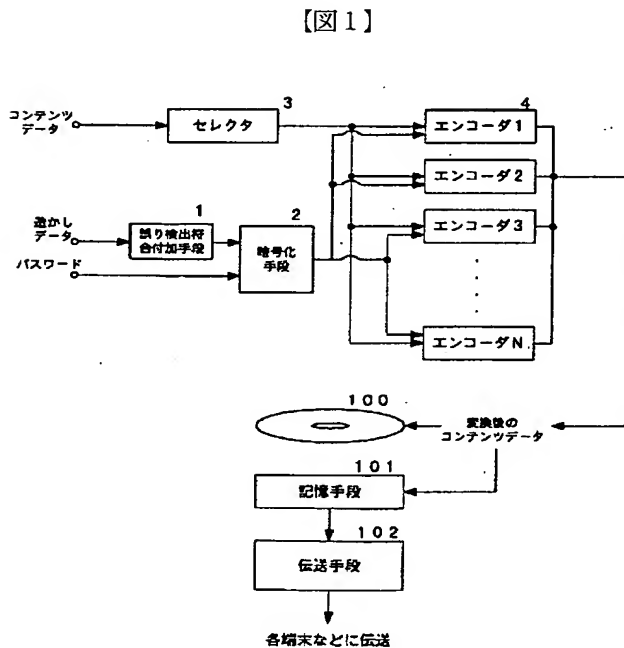
【0022】このように透かしデータを埋め込まれた変換後のコンテンツデータから透かしデータを読み出すために、図2に示す透かしデータ読み出し装置を使用する。同図によれば、変換後のコンテンツデータはN個のデコーダ5によって複数定義されている全ての透かしデータ読み出し方法に従って読み出される。そして読み出された仮の透かしデータは、ユーザーによって入力されたパスワードに基づいて復号化手段6によって復号化される。復号化された仮の透かしデータは、透かし埋め込み時に付加した誤り検出符号を利用して誤り検出手段7によって評価され、正当であると見なされた仮透かしデータをデータ選択手段8によって選択し、これを真の透かしデータを埋め込まれたコンテンツデータとして出力する。

【0023】

【発明の効果】以上説明したように、本発明に係る透かしデータ埋め込み装置、透かしデータ埋め込み方法、記録媒体、伝送方法、及び透かしデータ読み出し方法によれば、第三者による透かしデータに対する攻撃を想定した場合に、透かしデータを暗号化するためのパスワードを知らない限り、コンテンツデータに対して、どの程度の強度で透かしデータが埋め込まれているかを断定できないので、可能性のある最も強い強度の全てのコンテンツデータに対して攻撃を余儀なくされ、攻撃後のコンテンツデータの品質劣化が大きくなってしまいます。すなわち、パスワードを知らない限り、コンテンツデータから透かしデータだけを効率的に除去することができなくなるという効果がある。

【図面の簡単な説明】

【図1】本発明に係る透かし情報埋め込み装置の概念を

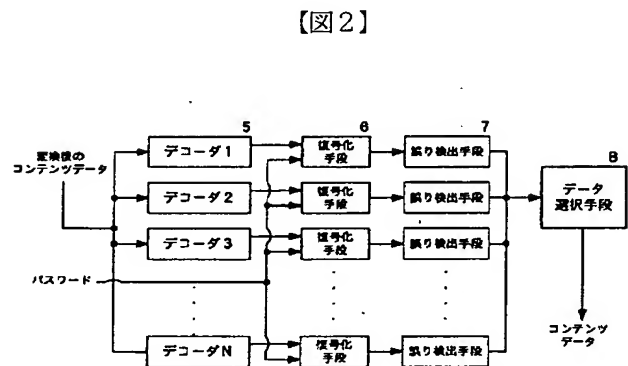


示すブロック図である。

【図2】本発明に係る透かし情報読み出し装置の概念を示すブロック図である。

【符号の説明】

- 1 誤り検出符号付加手段
- 2 暗号化手段
- 3 セレクタ
- 4 エンコーダ
- 5 デコーダ
- 6 複合化手段
- 7 正当性チェック手段
- 8 データ選択手段
- 100 記録媒体
- 101 記憶手段
- 102 伝送手段



フロントページの続き

(51) Int. Cl. 7

識別記号

F I

テーマコード(参考)

H 0 4 L 9/32

G 0 6 F 15/66

B 9 A 0 0 1

H 0 4 N 1/387

H 0 4 L 9/00

6 7 3 A

F ターム(参考) 5B057 BA26 CA12 CA16 CB12 CB16  
CB19 CC03 CE08 CE09 CG07  
CH08 CH18 DA17  
5C076 AA14 BA05 BA06  
5D044 AB05 AB07 CC04 DE17 DE52  
DE70 GK17  
5D378 QQ01 QQ11 QQ38  
5J104 AA07 AA14 KA01 NA05  
9A001 EE02 EE03 JJ19 LL03